Remarks

Reconsideration is requested in view of the preceding amendments and the following remarks.

Rejections under 35 U.S.C. § 101

Claims 1-5 stand rejected as being claims directed to a computer listing *per se*. Applicants respectfully traverse, but to expedite prosecution have amended claim 1 to clarify that the claims pertain to a hardware module.

Claim 18 stands rejected as allegedly not setting forth any steps. This rejection is traversed. Claim 18 depends from claim 17 and thus includes the steps recited in both claims 16-17. Withdrawal of this rejection is requested.

Rejections under 35 U.S.C. § 112

Claims 1-21 stand rejected as alleged being indefinite for the recitation of a "field-representation-select input." This rejection is traversed. For clarification, the expression "field-representation-select input" is amended as "field-type input." This expression means just what it says: an input used to select which type of field is to be used (i.e., a prime field or a binary extension field).

Claims 8-11 allegedly contain a number of relative terms that are either not defined in the claims or in the specification sufficiently to apprise one of ordinary skill in the art of the scope of the claims. This rejection is traversed, but to expedite prosecution and without change in claim scope, definitions have been added to claims 8 and 11.

Claim 18 is allegedly indefinite as failing to set forth any steps. This rejection is traversed. Claim 18 depends from claim 17 and thus includes the steps recited in claims 16-17.

The rejections under 35 U.S.C. § 102 and 35 U.S.C. § 103 set forth in the Office action are addressed below. For convenience, the paragraph number associated with each rejection is provided.

Rejections under 35 U.S.C. § 102

Claims 6-7 and 16-18 (paragraph 39)

Claims 6-7 and 16-18 stand rejected as allegedly anticipated by Monier, U.S. Patent 5,745,398 ("Monier"). This rejection is traversed.

Claim 6 recites a cryptographic processor, comprising:

> inputs for receiving a first and a second cryptographic parameter represented as elements of a finite field; and
> a multiplication module configured to receive the cryptographic parameters from the inputs, the multiplication module including at least two processing units configured to determine a Montgomery product of the cryptographic parameters, each processing unit receiving a bit corresponding to the first parameter and partial words of the second parameter.

Monier does not teach or suggest such a cryptographic processor. According the Office action, Monier's Fig. 1 shows a cryptographic processor that include inputs for first and second cryptographic parameters (Monier's *A* and *B*), and multiplication circuits 19, 20 that receive a bit of the first parameter and partial words of the second parameter. Applicants respectfully disagree. As inspection of Monier's Fig. 1 illustrates, Monier's multiplication circuit 19 is capable of receiving a bit of the parameter B and a word of the parameter A, but the multiplication circuit 20 does not receive a bit of the parameter B or a word of the parameter A,

and thus Monier's multiplication circuits 19, 20 do not correspond to the claimed processing units. Accordingly, claim 6 and dependent claims 7-11 are properly allowable over Monier.

Claim 16 recites a method of Montgomery multiplication that includes, in part:

> determining an intermediate value of a contribution to the Montgomery product based on a first bit of the first cryptographic parameter and the words of the second cryptographic parameter in a first pipeline stage;
> determining intermediate values of contributions to the Montgomery product based on remaining bits of the first cryptographic parameter in respective pipeline stages that receive the words of the second cryptographic parameter and an intermediate value from a prior pipeline stage.

The cited portions of Monier do not teach or suggest any pipelines stages. Instead, Monier merely teaches processing of various parameters in a single stage by executing an instruction loop. See col. 6, lines 62-64. The cited portions of Monier (col. 6, line 62 to col. 7, line 46, and col. 9, lines 7-46) merely refer to executing instructions in a loop, and do not teach or suggest any pipeline stages. Applicants respectfully request that the exact portion or portions of Monier that teach or suggest pipeline stages be specifically identified. Because Monier does not teach or suggest any pipeline stages, claim 16 and dependent claims 17-18 are properly allowable.

Claims 1, 6, and 12 (paragraph 52)

Claims 1, 6, and 12 stand rejected as allegedly anticipated by EPS CypherCalc: The Cryptographer's Calculator ("EPS"). This rejection is traversed.

CypherCalc does not teach or suggest the combinations of features recited in any pending claim. For example, amended claim 1 recites:

> a first input and a second input configured to receive a first operand and a second operand, respectively, represented as elements of a finite field;
> an output configured to deliver a Montgomery product of the first operand and the second operand; and

a field-type input configured to select multiplication of the first and second operands based on a prime field or a binary extension field.

While CypherCalc can be used to calculate a Montgomery product of a first and a second operand, CypherCalc requires that all field elements be represented as integers modulo a prime number, i.e., as elements of a prime field $GF(p)$, wherein p is a prime number. CypherCalc apparently permits selection of the prime number p that is stored CypherCalc's "N" operand memory, so that the size of the prime field can be selected. CypherCalc does not teach or suggest representing field elements in any other way such as, for example, as elements of the binary extension field $GF(2^k)$. CypherCalc does not teach or suggest selecting different field representations, and claim 1 and dependent claims 3-5 are properly allowable over CypherCalc.

With respect to claims 6 and 12, the Office action states that a field representation input as claimed corresponds to a portion of EPS showing conversion of hex numbers to decimal numbers. Decimal and hex numbers do not represent field types, and claims 6 and 12 and their dependent claims 7-11 and 13-15 are properly allowable.

Rejections under 35 U.S.C. § 103

Claims 1-5, 12-15, and 19-21 in view of Monier and Glaser (paragraph 21)

Claims 1-5, 12-15, and 19-21 stand rejected as allegedly obvious from a combination of Monier and Glaser et al., U.S. Patent 6,397,241 ("Glaser"). This rejection is traversed.

Amended claim 1 recites, in part, a field-type input configured to select multiplication of the first and second operands based on a finite field selected from a prime field or a binary extension field. The Office action admits that Monier does not teach or suggest such a feature, but asserts that Glaser does at col. 2, lines 39-46 and col. 13, line 65 to column 14, line 32. Applicants respectfully disagree. These cited portions of Glaser teach storing, for example, data

values for a prime field or computing integer-modulo N multiplications or modular polynomial basis multiplications. While the elements of a field can be represented with integers or polynomials, Glaser does not teach or suggest an input configured to select a prime field or a binary extension field. Accordingly, claim 1 and dependent claims 3-5 are properly allowable.

Independent claim 12 recites, in part, a field-type input. As noted above, Glaser merely teaches field elements represented as polynomials or integers, and does not teach or suggest selecting an input configured to permit selecting different types of fields. Accordingly, claim 12 and dependent claims 13-15 are properly allowable.

Independent claim 19 recites, in part, a Montgomery multiplier comprising a field-type input for selection of arithmetic operations corresponding to a prime field or a binary extension field. As noted above, no combination of Monier and Glaser teaches or suggests an input for selecting arithmetic operations for a prime field of a binary extension field. Accordingly, claim 19 and dependent claims 20-21 are properly allowable.

Applicants note that a rejection of claims 9-10 and 17 may also have been intended (see paragraph 28) but such a rejection was not noted in the summary paragraph (see paragraph 21). Clarification is requested. These claims depend from allowable claims and are allowable for at least this reason.

Claims 8-11 in view of Monier, Glaser, and the admitted prior art (paragraph 44)

Claims 8-11 stand rejected as allegedly obvious in view of a combination of Monier and Glaser or admitted prior art. This rejection is traversed. These claims depend from allowable claim 6 and are allowable for at least this reason.

Claims 2-4, 8-11, and 19 in view of EPS and Brandstrom (paragraph 56)

Claims 2-4, 8-11, and 19 stand rejected as allegedly obvious from a combination of EPS and Brandstrom, U.S. Patent 4,322,577 ("Brandstrom"). This rejection is traversed. The rejection of claim 2 is moot in view of the cancellation of this claim without prejudice. Claims 3-4 depend from allowable claim 1, and claims 8-11 depend from allowable claim 6 and are allowable for at least this reason.

Claim 19 recites a Montgomery multiplier comprising a field-type input for selection of arithmetic operations corresponding to a prime field or a binary extension field. No combination of EPS and Brandstrom teaches or suggests such a feature. EPS merely teaches representing integers in decimal or hex format, and Brandstrom teaches representing elements of the field $GF(p^r)$ as matrices so that for any values p, r arithmetic operations are performed in the same manner. Thus, Brandstrom does not teach or suggest selecting arithmetic operations based on selection of a prime field or a binary extension field as claimed. Accordingly, claim 19 and dependent claims 20-21 are properly allowable.

Claims 5 and 13-15 in view of EPS and Iwamura (paragraph 65)

Claims 5 and 13-15 stand rejected as allegedly obvious from a combination of EPS and Iwamura, U.S. Patent 5,321,752 ("Iwamura"). This rejection is traversed. Claims 5 and 13-15 depend from allowable claims 1 and 12 and are allowable for at least this reason.

Claims 7 and 16 in view of EPS and Monier (paragraph 70)

Claims 7 and 16 stand rejected as allegedly obvious from a combination of EPS and Monier. Claim 7 depends from allowable claim 6 and is allowable for at least this reason.

Independent claim 16 recites, in part, determining an intermediate value of a contribution to the Montgomery product based on a first bit of the first cryptographic parameter and the words of the second cryptographic parameter in a first pipeline stage and determining intermediate values of contributions to the Montgomery product based on remaining bits of the first cryptographic parameter in respective pipeline stages that receive the words of the second cryptographic parameter and an intermediate value from a prior pipeline stage. No combination of Monier and EPS teaches such features. EPS fails to teach determining an intermediate value of a contribution to the Montgomery product as recited in claim 16. Monier fails to cure the deficiencies of EPS. Monier teaches only a single stage that receive bits of a first cryptographic parameter and words of a second cryptographic parameter (Monier's multiplication circuit 19), and Monier does not teach or suggest respective pipeline stages as claimed. Accordingly, claim 16 is properly allowable over any combination of EPS and Monier.

Claims 17-18 -in view of EPS, Monier, and Iwamura (paragraph 76)

Claims 17-18 stand rejected as allegedly obvious from a combination of EPS, Monier, and Iwamura. This rejection is traversed. Claims 17-18 depend from allowable claim 16 and are properly allowable for at least this reason.

Claims 20-21 in view of EPS, Brandstrom, and Iwamura (paragraph 79)

Claims 20-21 stand rejected as allegedly obvious from a combination of EPS, Brandstrom, and Iwamura. This rejection is traversed. Claims 20-21 depend from allowable claim 19 and are properly allowable for at least this reason.

Conclusion

In view of the preceding, all pending claims are in condition for allowance and action to such end is requested. If any issues remain, please do not hesitate to telephone the undersigned.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

By _____
Michael D. Jones
Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 595-5300
Facsimile: (503) 228-9446